

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT		1. CONTRACT ID CODE J	PAGE OF PAGES 1 OF 2
2. AMENDMENT/MODIFICATION NO. P00126	3. EFFECTIVE DATE SEE BLOCK 16C.	4. REQUISITION/PURCHASE REQ. NO. N3032004RC4N014	5. PROJECT NO. (If applicable)
6. ISSUED BY SPACE AND NAVAL WARFARE SYSTEMS COMMAND CONTRACTING OFFICER: 02-N DEBRA L. STREUFERT 2231 CRYSTAL DRIVE, SUITE 400 ARLINGTON, VA 22212-3721 PHONE: 703-685-5508	CODE N00039	7. ADMINISTERED BY (If other than Item 6) NCIS Physical COI	CODE
8. NAME AND ADDRESS OF CONTRACTOR (No., street, country, State and ZIP Code) ELECTRONIC DATA SYSTEMS CORPORATION 13600 EDS DRIVE HERNDON, VA 20171 ATTN: NMCI CONTRACTS		(X)	9A. AMENDMENT OF SOLICITATION NO.
CODE 1U305			9B. DATED (SEE ITEM 11)
FACILITY CODE		X	10A. MODIFICATION OF CONTRACT/ORDER NO. N00024-00-D-6000
			10B. DATED (SEE ITEM 11) 06 OCTOBER 2000

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

☐ The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers ☐ is extended ☐ is not extended.

Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended by one of the following methods:

(a) By completing items 8 and 15, and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA (If required)

ACRN TBD: 1741804 12TF 233 30320 0 068892 2D C4N014 303204L2331N \$4,873,945.00

13. THIS ITEM APPLIES ONLY TO MODIFICATIONS OF CONTRACTS/ORDERS. IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

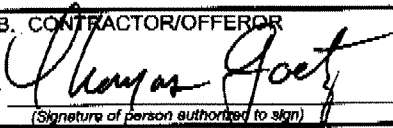

(X)	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.
	B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation date, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).
X	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF: FAR CLAUSE 52.212-4 (CHANGES)
	D. OTHER (Specify type of modification and authority)

E. IMPORTANT: Contractor ☐ is not, ☒ is required to sign this document and return (See Note below) copies to the issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)

Note: The Contractor may return a signed copy via facsimile or as a scanned image in portable document format (pdf).

-SEE HEREIN-

Except as provided herein, all terms and conditions of the document referenced in Item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.	
15A. NAME AND TITLE OF SIGNER (Type or print) THOMAS GOETZ, CONTRACTS MANAGER	16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print) A.L. DAVIS, CDR, SC, USN, CONTRACTING OFFICER
15B. CONTRACTOR/OFFEROR BY  (Signature of person authorized to sign)	15C. DATE SIGNED 30 SEP 04
16B. UNITED STATES OF AMERICA BY  (Signature of Contracting Officer)	16C. DATE SIGNED 30 SEP 04

- a. This modification is issued to add to Part One, Table Four, SCLIN 0029KD for Naval Criminal Investigative Service Physical Community of Interest, as follows:

Item	Service	Quantity	Unit	Unit Price	Total Amount
0029KD	Naval Criminal Investigative Service Physical Community of Interest Services (Non-Severable, Completion Type)	1	LO	\$4,873,945	\$4,873,945

The Contractor shall provide services to support the Naval Criminal Investigative Service Physical Community of Interest in accordance with the document entitled Statement of Work, NCIS Community of Interest (COI), Version 1.9, dated September 30, 2004. For the purposes of Section 1.2.2 entitled "Equipment," if the Government chooses to purchase the equipment dedicated to this service, the equipment shall have a price of zero dollars (\$0.00) upon receipt of Approval to Operate (ATO) notification from NETWARCOM, Designated Approval Authority (DAA), subsequent acceptance of SCLIN 0029KD, and the contractor's receipt of payment of SCLIN 0029KD.

- b. A conformed copy of the revised contract is made a part of this modification as a result of the changes outlined herein.
- c. All other terms and conditions of contract N00024-00-D-6000 remain unchanged and in full force and effect.



Statement of Work

NCIS Community of Interest (COI)

September 30, 2004

Version 1.9

Naval Criminal Investigative Service (NCIS)
Code 15, IT Services Department
716 Sicard Street, S.E.
Washington Navy Yard
Washington, DC 20388

TABLE OF CONTENTS

- 1.0 INTRODUCTION**
 - 1.1 Scope
- 2.0 BACKGROUND**
 - 2.1 Objective
 - 2.2 Period of Performance
- 3.0 REQUIREMENTS**
 - 3.1 Requirements Overview
 - 3.2 Organizational Requirements
 - 3.2.1 Protection of Information
 - 3.2.2 Official Records Repository
 - 3.2.3 Sharing Information & Applications: CONUS & OCONUS
 - 3.2.4 Ready Mobility of NCIS Agents
 - 3.2.5 Collaboration & Interaction with Other Agencies
 - 3.2.6 Law Enforcement Partner Communications
 - 3.3 Basic User Service Requirements
 - 3.3.1 E-Mail Services
 - 3.3.2 Print Services
 - 3.3.3 Directory Services
 - 3.3.4 Unclassified Remote Access Services
 - 3.3.5 Existing Infrastructure
 - 3.3.6 Email & File Share Services
 - 3.3.7 Outlook Web Access (OWA)
 - 3.3.8 Retention of DON Electronic Records
 - 3.4 Communications Service Requirements
 - 3.4.1 Wide Area Network (WAN) Connectivity
 - 3.4.2 Local Area Network (LAN) Communication Services
 - 3.5 Systems Service Requirements
 - 3.5.1 Operational Support Services (OSS)
 - 3.5.2 Domain Name Server (DNS)
 - 3.6 Other Service Requirements
 - 3.6.1 Information Assurance Services
 - 3.6.2 Public Key Infrastructure (PKI)
 - 3.6.3 Privacy and Security Safeguards
 - 3.6.4 Data Access & Cryptology
 - 3.6.5 Real-time Access Controls
 - 3.6.6 Access to Backup Media
 - 3.6.7 Testing and Transition Requirements
 - 3.6.8 Personnel Security Clearances
 - 3.6.9 Service Level Agreements
- 4.0 ROLES AND RESPONSIBILITIES**
 - 4.1 Government Roles and Responsibilities
 - 4.2 Contractor Roles and Responsibilities
- 5.0 DELIVERABLES**
- 6.0 COST**
- 7.0 POINTS OF CONTACT**

1.0 INTRODUCTION

Naval Criminal Investigative Service (NCIS) is a worldwide military law enforcement organization whose mission is to prevent terrorism and other hostile attacks, protect sensitive data and critical systems from compromise, and reduce criminal activities within the Department of the Navy (Navy, DoN or Government). NCIS accomplishes this mission by conducting felony criminal investigations, counterintelligence activities, and managing DoN security programs. NCIS currently has approximately 1,900 employees worldwide, 1,600 of them are located in over 110 locations in the continental United States (CONUS) and aboard ships and carriers. Due to the nature of the investigations, they lead and the operations they perform, much of the data that NCIS deals with is highly sensitive in nature. Although the information is typically unclassified, it is often considered sensitive and requires special handling. The data privacy requirement, the need for active worldwide collaboration and the high mobility of the NCIS agent workforce significantly distinguish the agency from the general Navy population. They are defined as a Community of Interest (COI) with requirements distinct from that of the general Navy. The purpose of this Statement of Work (SOW) is to define the requirements for the secure information services solution for the NCIS COI.

1.1 SCOPE

This SOW addresses the requirements for the NCIS COI that will be established to support the unclassified computer services for NCIS personnel. By definition, the NCIS COI includes members that will not be part of the Navy's CONUS infrastructure, such as the NCIS OCONUS locations, CONUS locations not connected via Navy infrastructure, and other law enforcement/counter terrorism organizations. The activities in this SOW will commence with the issuance of a task order.

This document contains the following major sections:

- Introduction
- Background
- Requirements
- Roles & Responsibilities
- Deliverables
- Cost
- Points of Contact

2.0 BACKGROUND

The current NCIS information services environment achieves privacy through direct ownership and operations of all systems. Communications privacy is maintained through hardware and software Virtual Private Networks (VPN) using approved Navy

communications solutions, such as DISA circuits, existing Base LANs, commercial broadband offerings, and dial-up connectivity. In addition to its own systems, NCIS maintains secure connectivity to external agencies through various means. Effective May 1st 2003, the unclassified and secret network operations and desktop management were assumed by the Navy Marine Corps Intranet (NMCI) contract. Currently, no NMCI seats have been delivered to any NCIS locations.

2.1 OBJECTIVE

The objective is to deliver an accredited physical COI that meets NCIS requirements, provides access to NCIS applications, email, file share and print services that meet current applicable information assurance standards. It is expected that the services solution transition will minimize user impact and will not impair agency operations.

2.2 PERIOD OF PERFORMANCE

The period of performance for this effort commences on the date of issuance of a task order and will be deemed complete upon completion of all the work hereunder and acceptance by the Government of the final test report and delivery of all reports listed as deliverables. The completion date is April 30, 2005.

3.0 REQUIREMENTS

The contractor shall provide an accredited physical COI and all deliverables required hereunder as set forth in this document.

3.1 REQUIREMENTS OVERVIEW

The NCIS COI will be a logical grouping of users who require access to information that must not be made available to the general user population. This requirement is based on any combination of specific security constraints, geographical location, unique functional requirements, or unique command related relationships. NCIS attributes requiring a COI are personnel systems for handling Privacy Act data, geographically dispersed major claimants, and the handling of sensitive law enforcement information. The NCIS COI must provide a secure, dedicated environment to its sensitive data and applications. The design should be easily transportable to the NCIS SIPRNET environment. File share storage will aggregate at the NCIS COI level.

3.2 ORGANIZATIONAL REQUIREMENTS

3.2.1 PROTECTION OF INFORMATION

The information services solution shall ensure protection of NCIS unclassified, sensitive information in its law enforcement, counterintelligence, counter-terrorism, clearance adjudication, force protection, Privacy Act of 1974, grand jury, and financial

privacy activities and to continue to support its need to act as a unified global Navy command.

3.2.2 OFFICIAL RECORDS REPOSITORY

The information services solution shall support the NCIS role as an official records repository for the entire Department of the Navy, as established by SECNAVINST 5580.1.

3.2.3 SHARING INFORMATION & APPLICATIONS: CONUS & OCONUS

The information services solution shall allow all NCIS detachments to act as a global organization and share information and applications centrally. NCIS COI users serviced by the contract must be able to share information and applications with their OCONUS detachments.

3.2.4 READY MOBILITY OF NCIS AGENTS

The information services solution shall support the ready mobility of employees inside and outside of the CONUS Navy infrastructure. The contractor shall provide a NCIS COI solution that fully supports the rapid deployment of task forces and other NCIS operational teams to both NCIS and non-NCIS environments.

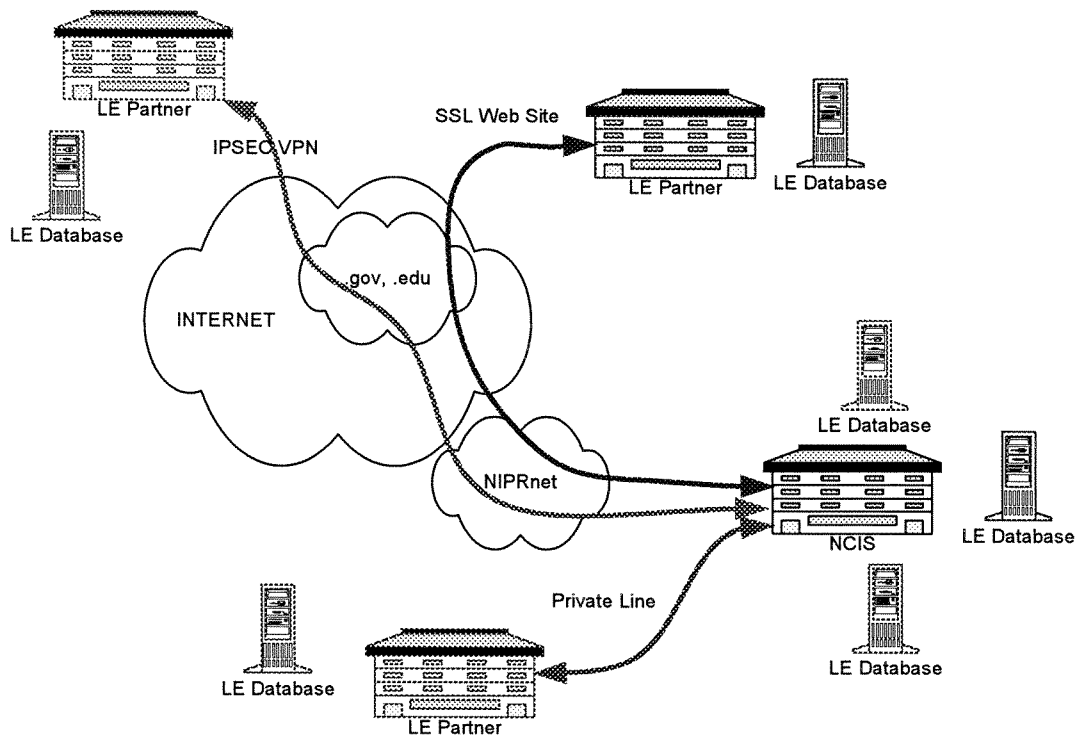
3.2.5 COLLABORATION & INTERACTION WITH OTHER AGENCIES

The contractor shall provide a solution that gives NCIS the ability to share information and collaborate in a secure environment with their counterparts at other Federal, state and local agencies, and access both internal and external data repositories and networks after transitioning to the NCIS COI. The contractor shall ensure that the NCIS data center maintains the capability to connect to the NIPRNet and allow non-COI users access to its resources.

3.2.6 LAW ENFORCEMENT PARTNER COMMUNICATIONS

The contractor shall provide a solution that will fully support the current and future connections between NCIS and partner law enforcement organizations as shown in the drawing below.

NCIS Law Enforcement Partner Connection Models



3.3 BASIC USER SERVICE REQUIREMENTS

The contractor shall provide a solution that must inter-operate with, and deliver service levels consistent with, the NMCI basic user services and provide access to legacy NCIS applications.

3.3.1 E-MAIL SERVICES

The contractor shall provide services for sending, storing, processing, and receiving e-mail and multi-media e-mail attachments, with interoperability across DoN and within the DoD. The services shall be configurable to provide capability for sending and receiving signed and encrypted e-mail and attachments, by utilizing DoD PKI (Public Key Infrastructure) issued user certificates, and interoperable with systems outside the Navy domain. Service shall be provided with e-mail packages that support cryptographic functions from a smart card.

E-Mail access must include the functionality to send/receive, access local contacts and Navy GAL for addressing, moving e-mail to PSTs (on Navy network file share or local machine), synchronization or other method to have an e-mail on both the exchange server and the desktop. This must also include the capability to interface with a contractor provided, or NCIS provided, Blackberry enterprise server.

The contractor will ensure that foreign nationals are clearly identifiable in electronic communications in accordance with DoD Directive 5230.20. This solution also includes access controls, back up and recovery.

3.3.2 PRINT SERVICES

The contractor's solution shall provide an accredited print solution to all NCIS COI users. NCIS print data streams may not reside on servers or pass through networks outside of NCIS control unless encrypted. Notwithstanding the foregoing, the Government acknowledges that at least thirty-five (35) existing print servers are subject to the Exchange/Sale Authority (Section 6.23) and the contractor will provide any additional required print servers beyond those print servers transferred to the contractor as part of the Exchange/Sale Authority to satisfy the current configuration of NCIS deployed users.

3.3.3 DIRECTORY SERVICES

The contractor shall integrate with the Navy global information services to deliver a distributed computing environment that supports the management and utilization of file services, network resources, security services, messaging, web, e-commerce, white pages, and object-based services, across the NCIS COI. Information services shall include storing, updating, and publishing directory information from multiple systems and formats including e-mail addresses, commercial and DSN telephone numbers, certificates, addresses, applications, network devices, documentation, and routing information, as well as other data/resources in support of the Navy IT environment. The contractor shall ensure directory entries conform to Government standards and provide the flexibility to include DoN users not directly supported by Navy in directory services.

The global directory services shall be required to maintain information on users and resources. The DS should support and facilitate the following basic functions:

1. Supported by PKI authentication services, provide the capability for users, devices, and applications to discover and utilize global information services data.
2. Support the monitoring of administration and management of network resources.
3. Support the implementation of global account management and subsequent authentication and authorization to data maintained in the global directory service.
4. Support the enablement and distribution of applications.
5. Provide a proactive environment that builds and manages relationships between objects within the global directory service.
6. Support the ability for end users to interact globally (anywhere, anytime) with the network directory services in a transparent and consistent manner.

3.3.4 UNCLASSIFIED REMOTE ACCESS SERVICES

The contractor shall ensure that users can access the NCIS data network from remote locations via the Navy remote access service.

3.3.5 EXISTING INFRASTRUCTURE

The contractor shall provide a solution that leverages existing Navy/NCIS file and email services, and any other applicable infrastructure, to include software licenses, wherever possible.

3.3.6 EMAIL & FILE SHARE SERVICES

The contractor shall provide a solution that provides all NCIS employees standard MS Outlook access to email and common access to file share services. The email access must include functionality to: send and receive messages; access local contacts; access the NCIS and Navy Global Address List (GAL). NCIS must be able to control access to NCIS data.

3.3.7 OUTLOOK WEB ACCESS (OWA)

The contractor will provide capability which allows access to Navy e-mail via OWA using appropriate authentication via a third party maintained hardware/software entry point with a browser compatible with Secure Sockets Layer (SSL).

3.3.8 RETENTION OF DON ELECTRONIC RECORDS

The contractor shall provide retention of electronic information files consistent with applicable DoD (DoD Standard 5015.2-STD) and DON policy (SECNAVINST 5212.5D).

3.4 COMMUNICATIONS SERVICE REQUIREMENTS

The contractor shall provide communications services with security features in accordance with the requirements in the following subparagraphs.

3.4.1 WIDE AREA NETWORK (WAN) CONNECTIVITY

The contractor shall provide all services required to attain wide area network (WAN) connectivity between geographically separated NCIS users/devices. It provides connection to external networks, to include but not be limited to: Non-Secure IP Router Network (NIPRNET), Defense Research Engineering Network (DREN), Defense Switched Network (DSN), Public Switched Telephone Network (PSTN), and the Internet. The WAN solution shall incorporate the Government-Service Provider agreement for DISA connectivity.

The contractor shall provide for operation and maintenance of the VPN connection between the Norfolk and San Diego Network Operation Centers and the Transport Access point located at the WNYD.

3.4.2 LOCAL AREA NETWORK (LAN) COMMUNICATION SERVICES

The contractor shall ensure that the solution integrates with Navy and Marine Corps Local Area Networks (LANs) and Base Area Network (BAN) attached devices.

3.5 SYSTEMS SERVICE REQUIREMENTS

3.5.1 OPERATIONAL SUPPORT SERVICES (OSS)

The contractor solution must provide for the future implementation of a NMCI Network Operations display that will allow for the real-time monitoring of network assets. Upon implementation, the display would be available to authorized users at any mission-critical seat and show performance status of the overall network and individual servers and routers. Custom components provided under this contract must be included on the network operations display, ordered via a separate Task Order.

During this effort, the contractor shall provide services that include, but are not limited to, Data Backups and Recovery, Data Archiving, Routine Database Audits and Maintenance, Log Retrieval and Audits, Purging of Records, and Network Address Administration. The contractor shall support Government oversight, maintain accessible historical data, and provide summary management information that details the OSS functions. The contractor also shall demonstrate these capabilities to the Government prior to acceptance of this task order.

3.5.2 DOMAIN NAME SERVER (DNS)

The contractor shall integrate with the Navy Domain Name Server (DNS) services that include the address resolution of Uniform Resource Locator (URL) to IP addresses. This capability shall include internal Navy and Marine Corps URLs as well as external URLs. The services shall meet all functionality of the current Domain Name Server (DNS) service, to include flexible support for deployed units and retain the navy.mil and usmc.mil domain naming conventions.

3.6 OTHER SERVICE REQUIREMENTS

3.6.1 INFORMATION ASSURANCE SERVICES

As specified in DoD 5200.28 (Security Requirements for Automated Information Systems (AISs), DoDI 5200.40 (DoD Information Technology Security Certification and Accreditation Process -DITSCAP), SECNAVINST 5239.3, OPNAVINST 5239.1B, and DoD 5200.2-R, all automated systems shall meet fundamental security requirements and must be accredited by the Designated Approving Authority (DAA) prior to processing classified or sensitive non-classified data. The NCIS COI shall be implemented with proper products, policies, and procedures to ensure required system C&A in accordance with this policy. In addition, the specific IA guidelines specified in

CNO ALCOM 081949Z SEP 99, DoN CIO ITIA, and DoN ITSG shall be implemented within the NCIS COI.

3.6.2 PUBLIC KEY INFRASTRUCTURE (PKI)

As specified in DEPSECDEF Memo of 09 Apr 1999, DoD PKI Implementation, any PKI employed within DoD Services and Agencies shall be the DoD PKI. Thus, the NCIS COI shall incorporate DoD PKI in accordance with the following guidelines. Specifically, the high assurance PKI based in FORTEZZA and the medium assurance PKI based on X.509 Version 3 certificates shall be used within the NCIS COI. The Government will provide the Contractor with the DoD PKI user profile as GFI to be implemented within the NCIS COI. The Contractor shall support the medium assurance PKI implementation of smart cards. In accordance with DEPSECDEF memo of 10 November 1999, the primary carrier of the DoD medium assurance PKI credentials will be the Common Access Card (CAC), a smart card.

Based on this policy, the NCIS COI contractor shall:

- a. Use only DoD Public Key Infrastructure (PKI)-enabled email and file share servers.
- b. Provide digital signature capability for all electronic mail services implemented. The DoD PKI credentials will be residing on the CAC or equivalent DoN provided smart card.
- c. Register email and file share servers and install DoD PKI server certificates for PKI enabled applications DoD PKI certificates will be used for client-server identification and authentication for all private DoD and DoD-interest web servers on both classified and unclassified networks.

3.6.3 PRIVACY AND SECURITY SAFEGUARDS

The contractor shall not publish or disclose in any manner, without written consent of the Government the details of any security safeguards delivered hereunder.

The contractor shall deliver procedures and implementation plans to ensure that IT resources leaving the control of the assigned user, such as being reassigned, removed for repair, replaced, or upgraded, is cleared of all DoN data and sensitive application software by a technique approved by the Government, currently overwriting at least three times. For IT resources leaving DoN use, applications acquired via a "site-license" or "server license" shall be removed. Damaged IT storage media shall be degaussed or destroyed. To the extent required to carry out a program of inspection and audit to safeguard against threats and hazards to the confidentiality, integrity, and availability of Government data, the contractor shall afford DoN access to the contractor's facilities, installations, technical capabilities, operations, documentation, records, databases, and personnel.

3.6.4 DATA ACCESS & CRYPTOLOGY

The contractor shall provide a solution that ensures that all NCIS information is cryptologically separated from all other Navy data traffic and will never be transmitted on any LAN or WAN segment that could be exposed to unauthorized personnel unless encrypted in transit.

3.6.5 REAL-TIME ACCESS CONTROLS

Unauthorized users/contractors must not be able to access unencrypted e-mail and file shares without a real time intrusion detection system being placed on the servers to notify NCIS that such access is occurring. The Contractor shall provide NCIS the capability to monitor independently access to the NCIS COI.

3.6.6 ACCESS TO BACKUP MEDIA

During this effort, access to unencrypted backup media must be restricted to authorized Government employees or appropriately screened contractor personnel. The backup media containing unencrypted data must be delivered daily to an authorized Government employee and handled in accordance with current Navy and NCIS directives regarding handling of sensitive information. These backup media must be restricted to containing only NCIS COI data.

3.6.7 TESTING AND TRANSITION REQUIREMENTS

The contractor shall demonstrate that the COI meets all NCIS requirements and provide test criteria and scenarios, at the below pilot sites to validate that the information services solution meets or exceeds all of the NCIS stated requirements. These pilot sites represent a cross section of NCIS site types and communications abilities and should be coordinated with NMCI transition managers.

NCISHQ Building 111, 176, 218, WNY
NCISRA Lemoore
NCISRA Ventura
NCISRA Charleston
NCISRU Lakehurst
NCISRU Mechanicsburg
NCISRU NAF Andrews, AFB

Washington, DC
Lemoore, CA (SWLM)
Port Hueneme, CA (SWPH)
Charleston, SC (CACS)
Lakehurst, NJ (NELH)
Mechanicsburg, PA (NEMB)
Camp Springs, MD (DCAD)

Upon mutual agreement, final pilot locations may change dependant upon NMCI and Non-NMCI network readiness. The Government will identify a primary and alternate POC for each site within thirty (30) days of scheduled pilot performance. Notwithstanding the foregoing, an onsite engineering presence will be available at the Washington Navy Yard but may not be present at all pilot sites.

Using the service level agreements set forth in the DoN NMCI contract N00024-00-D-6000, dated 6 October 2000, as appropriate, the contractor shall deliver the

performance testing criteria and scenarios, with Government assistance. It is anticipated that upon successful completion of test scenarios, users at the above site will continue to exercise the provided solutions in their operational environments for a minimum two (2) weeks, not to extend beyond April 30, 2005, to ensure continued success using COI resources. Contractor will be responsible for the correction of any deficiencies identified during either these test periods.

The contractor shall deliver the organizational transition plan to the approved solution.

The contractor shall deliver an interoperability test plan and procedures that will minimize the possibility of problems during modification of user existing configurations, verifies that interoperability is intact upon completion of the modifications, and provides for interoperability monitoring during service provisioning.

The contractor shall ensure that interoperability between the NCIS COI and all existing non-NCIS COI GIG components including those defined in the OA, is maintained during the modification. The contractor's Interoperability Test Plan shall verify interoperability after segment installation and integration completion. As part of post modification testing, Interoperability Testing shall include, but is not limited to, a verification of the interoperability of the joint and DOD wide applications that are legacy to the segment being modified. The Government testing and evaluation plans will define the applications and other critical applications that are legacy to the segment being installed and integrated or modified. The Government providing of a list of critical applications for interoperability assurance and testing purposes does not alleviate the contractor of the contract requirement to maintain the interoperability of legacy applications. The Interoperability Test plan shall also provide for a series of mechanisms that detect unacceptable trends in performance that indicate that the software and hardware installed, component settings, and/or procedures are not in compliance, and must be corrected to support interoperability. This test plan shall address availability as it relates to the following services:

- Standard Office Automation Software
- E-mail Services
- Directory Services
- Web Access Services
- Newsgroup Services
- NCIS COI Intranet Performance
- NIPRNET Access
- Internet Access
- Desktop Access to Government Applications
- Unclassified Remote Access
- Organizational Messaging Services
- Wide Area Connectivity
- BAN/LAN Communications Services
- External Networks

- Public Key Infrastructure (PKI)

The test plan reporting criteria shall include a threshold level, agreed to by Government and the contractor, that requires immediate notification of the Government and appropriate action by the contractor to correct. Corresponding SLAs are prescribed for these services and they stipulate response times to Government for exceeding these threshold levels and correcting NCIS COI related deficiencies. The test plan will be proposed by the contractor and approved by the Government.

3.6.8 PERSONNEL SECURITY CLEARANCES

The contractor shall ensure that all of the contractor's personnel with access to NCIS data shall carry a minimum of a SECRET clearance with additional Law Enforcement screening to be provided by NCIS.

The contractor shall ensure that only NCIS authorized personnel are able to access unencrypted sensitive information contained anywhere on its network, systems, and data that are generated by NCIS, as well as data received or extracted from other law enforcement agencies and databases. Cleared NCIS personnel must escort all contractor personnel requiring access to SCIFs.

3.6.9 SERVICE LEVEL AGREEMENTS

No SLA's will apply to this requirement (SCLIN 0029KD).

4.0 ROLES AND RESPONSIBILITIES

4.1 GOVERNMENT ROLES AND RESPONSIBILITIES

- Government arranged site access (including escorts when required) for contractor personnel.
- NCIS is responsible for control of access to legacy applications.
- NCIS is responsible for control of access to collaborative environments that support the COI.
- NCIS is responsible for physical control of unencrypted email and file share environments that support the COI.
- NCIS is responsible to ensure all servers and network components owned or leased by NCIS remain operational, as necessary.
- NCIS user will properly identify himself or herself to the Help Desk representative.
- NCIS shall provide the contractor with the names of NCIS COI users. NCIS will provide keywords to the Help Desk representatives to support verification of NCIS COI user status. NCIS shall provide and implement training backed by policy to NCIS COI users on NCIS COI user verification status.

- NCIS will provide training to all NCIS COI users on the safe handling of sensitive law enforcement data.
- NCIS must provide a list of personnel requiring email notification of unauthorized personnel accessing their data.
- The end user is responsible for, and must prevent, For Official Use Only (FOUO) information from remaining in a temporary file or web cache.
- NCIS will fund the additional requirement for law enforcement screening of contractor's personnel.
- NCIS will supply adequate physical space in its server farm to accommodate the contractor's servers and other equipment supporting the NCIS COI operations. The space will be located in Bldg. 111, on the Washington Navy Yard and will be suitable for its intended use (ie, environmental support and hardening are in place).
- NCIS will be responsible for inventorying and destruction of any media that houses NCIS data.
- NCIS will ensure all data is removed from local data storage device (hard drive) before the device is removed for repair or replacement.
- NCIS will provide a technical liaison and appropriate documentation to support the contractor's efforts.
- The Government will provide timely delivery of Government Furnished Equipment/Information (GFE/I), and will be responsive to scheduled meetings, reviews, and draft deliverable turnarounds.
- All network addressing in the DMZ extension is the responsibility of the legacy domain.
- Layer 3 addressing for the servers located in the DMZ extension will be independent of NMCI.
- NCIS must ensure that all non-NCIS COI personnel requiring data or collaboration resources from the DMZ extension have the proper authentication to access the data.

4.2 CONTRACTOR ROLES AND RESPONSIBILITIES

- The contractor will adhere to restrictions with respect to accessing system backup media. Such access will be restricted to authorized NCIS employees or appropriately screened personnel only.
- The contractor will provide all hardware, software, and services required to demonstrate and satisfactorily implement the NCIS COI solution.
- SLAs shall only apply to operations associated with NCIS COI users when physically located within CONUS.
- The contractor shall have procedures to support verification of NCIS COI user status for user administration issues.
- The contractor shall have procedures to ensure consistent direction for user login under regular use as well as troubleshooting.

- The contractor will not co-mingle any other data on the back up tape for NCIS' data. Remote back up administrators from the NOC will be unable to see the NCIS data on the tapes.
- The contractor will draft a MOA to perform daily delivery of backup media.
- All NCIS COI users will be able to access email and file share services, it being understood that access by OCONUS NCIS users will be dependent upon availability of NIPRNET connectivity to those users.

5.0 DELIVERABLES

The primary deliverable of this task order is a NCIS COI that meets all NCIS requirements and successfully completes all tests outlined in this SOW. Additionally, the contractor will deliver the following:

- Requirements Document (w/ Traceability Matrix)
- Architectural Concept Document
- Test Plan (w/ scenarios, criteria, test results)
- Transition Plan
- Hardware security & maintenance procedures and plans
- Bi-Weekly Reports- The contractor shall provide the COR a Bi-Weekly Status and Performance Report. This report shall provide current status and details on work completed. In addition, this report shall indicate the progress and status of each task or project and identify any existing or potential problem areas. This report shall be in Microsoft Word 2000 format. This report is due to the COR by COB on the 2nd business day of the week following the two week period.
- Final Acceptance Test Report demonstrating compliance with all requirements of the SOW.

Upon submission of the foregoing deliverables, the Government will have ten (10) business days to review such deliverables. Failure to respond within the ten (10) day period will be considered acceptance of that deliverable. Any requested revisions on the part of the Government should represent corrections only.

Acceptance of the NCIS COI solution occurs upon receipt of Approval to Operate (ATO) notification from NETWARCOM, Designated Approval Authority (DAA).

6.0 COST

This is a firm fixed-price CLIN.

7.0 POINTS OF CONTACT

NCIS Technical Representative
 Mr. Jerry Dorsett, Chief, Network Division (15N)
 Naval Criminal Investigative Service (NCIS)
 716 Sicard Street, SE

Washington Navy Yard
Washington, DC 20388
Office: 202-433-3543

NCIS Coordinator for NMCI
Ms. Susan Russell
Naval Criminal Investigative Service (NCIS)
716 Sicard Street, SE
Washington Navy Yard
Washington, DC 20388
Office: 202-433-9305